A Judge Just Made It Harder for the FBI to Use Hacking

3-4 minutes

A judge has thrown out evidence obtained by the FBI via hacking, after the agency refused to provide the full code it used in the hack.

The decision is a symptom of the FBI using investigative techniques that are usually reserved for intelligence agencies, such as the NSA. When those same techniques are used in criminal cases, they have to stack up against the rights of defendants and are subject to court processes.

The evidence that was thrown out includes child pornography allegedly found on devices belonging to Jay Michaud, a Vancouver public schools worker.

Michaud was arrested in July 2015 as part of the FBI's investigation into dark web child pornography site Playpen.

In February 2015 the FBI took control of Playpen, and for just under two weeks ran it from a government server. During this time, the agency deployed what it calls a network investigative technique (NIT)—or a piece of malware—to identify the site's users.

The malware relied on a vulnerability in the Tor Browser that was used to break into targets' computers, before grabbing their IP address and other technical information.

In February, judge Robert J. Bryan ordered the FBI to reveal the full malware code to the defense under a protective order. One reason the defense wanted to examine the exploit and other NIT parts was to verify that the FBI did not go beyond the scope of the warrant.

Michaud's case has been a dramatic legal tussle, dealing with the balance between a defendant's right to information, and the government's interest in keeping sensitive investigative techniques under wraps.

The Department of Justice fought back against the order, largely in sealed filings, and asked the judge to reconsider.

After a private meeting with the government earlier this month, Judge Bryan changed his mind, and said the FBI did not have to turn over the exploit. But in a complicated legal wrinkle, he still thought the defense still had a right to see the malware code.

When the FBI refused, the judge tossed the evidence.

Short of a government appeal, the Michaud case may well be over.

Other judges have thrown out evidence in related cases but for different reasons. Last month, Judge William G. Young of the District of Massachusetts suppressed all evidence in a Playpen case because the warrant used to authorise the malware was void. Shortly after, another judge in Oklahoma did the same.

"We are disappointed with the decision and are reviewing our options," Department of Justice spokesperson Peter Carr told Motherboard in an email.